HMD (2017) 54:1–3
DOI 10.1365/s40702-017-0289-2

EDITORIAL

IT-Risikomanagement

Matthias Knoll

Online publiziert: 13. Januar 2017

In unserer Gesellschaft lässt sich ein Wandel beobachten, der seit einigen Jahren stetig fortschreitet und daher vielleicht nicht immer überall offensichtlich erkennbar ist: Die Digitalisierung der Wirtschaft und des Privaten.

Durch zunehmende Verfügbarkeit von Breitband-Internet, immer leistungsfähigeren Mobilgeräten und unzähligen anderen innovativen Technologien eröffnen sich für Unternehmen aller Größen und Branchen bislang unbekannte Möglichkeiten. Neue Geschäftsmodelle und neue Unternehmen entstanden und entstehen, Kundenbindung wird – etwa durch raffiniert gestaltete Dienstleistungen wie Software-Abo-Modelle oder vorausschauende Wartung – neu definiert.

In gleichem Maß ändern sich unsere Nutzungsgewohnheiten dieser Technologien und ihrer „Produkte“. An der einen Stelle schneller, etwa bei Smartphones oder den sogenannten Wearables wie Fitness-Tracker, vielleicht auch, weil der Druck des sozialen Umfeldes uns dazu zu zwingen scheint. An anderer Stelle langsamer, etwa bei Smart Home, das ob vieler konkurrierender Standards und verschiedener technischer Implikationen nur zögerlich in Privathaushalte Einzug hält.

Doch der Trend zu immer mehr IT, zu einer Internet-basierten allumfassenden Vernetzung von Menschen *und* Maschinen und damit zu einer nicht nur gefühlt wachsenden Abhängigkeit von der IT ist unaufhaltsam. Einige Beispiele: Neueste Cloud-Technologie als schneller Überall-Dabei-Datenspeicher und flexible Plattform für Anwendungen verändert die Arbeitswelt, Unternehmensgrenzen und ortsfeste Arbeitsplätze lösen sich auf. Die Energiewende führt zu einer Dezentralisierung der Stromnetze und damit zu neuen Regelungs- und Verteilmechanismen, die nur mit IT-Unterstützung realisiert werden können. Aus dem Bahn- und Flugverkehr ist IT schon lange nicht mehr wegzudenken. Der Straßenverkehr in großen Städten

M. Knoll (✉)
Hochschule Darmstadt, Darmstadt, Deutschland
E-Mail: matthias.knoll@h-da.de

und die Wasserversorgung werden mittlerweile zentral gesteuert. In Krankenhäusern und Arztpraxen fließen hochsensible Daten durch das Netzwerk, sind Diagnose- und Therapiegeräte miteinander und mit den Computern der Verwaltung vernetzt. Die gesamte Finanzwelt stünde ohne IT still. Unternehmen steuern mit Hilfe der IT die weltweite Produktion und Produktionslogistik, Anlagen, die bislang autark arbeiteten, sind nun miteinander verbunden und liefern Daten über sich selbst und das Ergebnis ihres Tuns. Das ist hilfreich für das eigene Unternehmen, aber auch die Herstellerfirma, die darüber neue Geschäftsmodelle realisieren kann.

Das all diese Themen umfassende Stichwort „Smart" verspricht eine schöne neue Zukunft, in der das Leben leichter und die Möglichkeiten vielfältiger sein werden.

Doch ist das wirklich so? Allzu gerne werden bei solchen Szenarien mögliche Risiken in den Hintergrund gedrängt. Denn Risiken sind „Spielverderber".

Also besser nicht thematisieren, es trifft ohnehin nicht das eigene Unternehmen oder den eigenen Haushalt? Wer soll sich schon für „mein" Unternehmen oder die persönlichen Daten auf meinem PC im häuslichen Arbeitszimmer interessieren? Man hat nichts zu verbergen, ist vermeintlich nicht wichtig und deshalb kein lohnendes Angriffsziel.

Diese Argumente klingen vielleicht vertraut. Doch kann, darf man sich von der Thematik in dieser Form abwenden? Sicherlich nicht.

Noch ist der „Sündenfall" nicht eingetreten. Zwar gab es auch in der jüngeren Vergangenheit verschiedene Vorfälle, von denen einer zuletzt sogar die Bundeskanzlerin vor die Kameras und Mikrofone holte, weil er Hunderttausende Privathaushalte betraf. Da wird IT dann rasch in die Nähe der inneren Sicherheit gerückt. Auch warnen Politiker, Sicherheitsbehörden, Wissenschaftler und Institutionen wie etwa der Chaos Computer Club eindringlich vor möglichen Gefahren und schlagen unterschiedliche Strategien zur Beherrschung vor. Doch noch ist keines der von Sicherheitsexperten skizzierten denkbaren Katastrophenszenarien eingetreten. Das verschafft uns allen jedoch bestenfalls ein wenig Zeit.

Während viele größere Unternehmen mittlerweile die Brisanz erkannt und ein leistungsfähiges IT-Risikomanagement installiert haben, besteht insbesondere im Mittelstand, bei kleinen Unternehmen und vor allem im Privaten Aufklärungs- und Nachholbedarf.

Denn gutes IT-Risikomanagement ist keine Aufgabe für einige wenige Experten. Gutes IT-Risikomanagement geht uns alle an. Ohne Ausnahme. Als Teil der Belegschaft tragen wir unseren Teil der Verantwortung ebenso wie als Nutzer im Privaten. Niemand möchte, dass Einbrecher unser Zuhause heimsuchen und genauso müssen wir unser digitales Zuhause und unser digitales Ebenbild im virtuellen Raum gegen Eindringlinge und Missbrauch absichern. Um an dieser Stelle möglichen Missverständnissen vorzubeugen: Es geht nicht um die Verbreitung von Pessimismus oder Angst. Wir alle können von der IT und ihren neuen Möglichkeiten in unterschiedlicher Form profitieren. Aber wir müssen uns unserer Verantwortung bewusst sein, den Gedanken an Risiken im Kontext des Digitalen mehr Raum geben und Zusammenhänge hinterfragen. Wir müssen uns selbst ebenso wie die Hersteller und Anbieter von Produkten und Dienstleistungen stärker in die Pflicht nehmen. Technische und vor allem auch nicht-technische Ansätze und Ideen zur Beantwortung der damit einhergehenden komplexen Fragen gibt es bereits. An sie kann und muss an-

geknüpft werden. Unser Ziel muss es sein, immer umfassender proaktiv statt reaktiv zu handeln, um unsere digitale Freiheit erfolgreich verteidigen zu können.

Die vorliegende Ausgabe der HMD zum Thema IT-Risikomanagement gibt im Überblicksbeitrag und acht weiteren Schwerpunktbeiträgen Impulse für die Arbeit mit Risiken aus der und für die Informationstechnologie.

Der Bogen ist weit gespannt von Detailfragen zum Risikomanagement-Prozess über eine Betrachtung relevanter Vorgaben hin zu Fragen des Datenschutzes und zum Umgang mit den eigenen Daten. Weiterhin ergänzen Beiträge zur Behandlung von Risiken im Kontext von Industrie 4.0 und der Cloud, zur Effizienzbewertung bestimmter Maßnahmen sowie zur Beherrschung von Risiken im Kontext der berüchtigten „Schatten-IT“ das Themenfeld.

Zwei weitere Beiträge im Spektrum zum Thema Fraud Detection im Gesundheitswesen sowie der veränderten Softwarenutzung runden die Ausgabe ab.

Besonders interessant im Kontext des IT-Risikomanagements mag vielleicht die Rezension des Titels „Unternehmenseigene Ermittlungen“ und des darin enthaltenen Kapitels „IT-Forensik“ sein.

Mein herzlicher Dank gilt allen Autorinnen und Autoren dieser Ausgabe, die ihr Wissen mit Ihnen teilen und so wertvolle Impulse für die Diskussion geben. Ich wünsche Ihnen eine spannende Lektüre, aus der Sie viel Wissen mitnehmen können und freue mich über Ihr Lob, Ihre Anregungen und Ihre Kritik.

Nochmals aufgreifen wollen wir das Thema demnächst in der Buchreihe Edition HMD. Meine Mitherausgeberin Prof. Susanne Strahringer (TU Dresden) und ich planen ein Buch mit dem Titel „IT-GRC-Management“, das sich – natürlich – auch dem Thema Risiko zuwenden wird.

Wer sich mit einen Beitrag zu einem der drei Themenfelder einbringen möchte, ist herzlich eingeladen, sich an uns zu wenden.